19/5/5 (Item 5 from file: 347)
DIALOG(R)File 347:JAPIO

05650716 **Image available**
PROCESSOR FOR PREPAID IC CARD

PUB. NO.: 09-265516 [JP 9265516 A]
PUBLISHED: October 07, 1997 (19971007)
INVENTOR(s): NISHIOKA MITSURU
APPLICANT(s): TOSHIBA CORP [000307] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-076201 [JP 9676201]
FILED: March 29, 1996 (19960329)
INTL CLASS: [6] G06K-017/00; A63F-007/02; G07F-007/08; G07F-007/12
JAPIO CLASS: 45.3 (INFORMATION PROCESSING -- Input Output Units); 29.4 (PRECISION INSTRUMENTS -- Business Machines); 30.2 (MISCELLANEOUS GOODS -- Sports & Recreation)

ABSTRACT

PROBLEM TO BE SOLVED: To prevent a secret key, etc., from being leaked, or stolen and illegally used, or illegal use through an alteration of a subtracting machine, etc., by registering collation data from a 2nd IC card in a handling means, and judging the propriety of a 1st IC card which has operation data enabling normal operation on the basis of the collation data.

SOLUTION: An operator inserts a registration card into equipment. When the inserted card is a registered and 'rewriting' is permitted by setting and data are not registered, the equipment side perform mutual authentication for confirming the propriety of the card. When the result is OK, an inputted password code is matched so as to confirm the propriety of the user, and then the registered data beings to be read for the 1st time after OK is obtained. When the password number is NG, data are not outputted even if a read of the data from the card is tried. The data which are thus read out are stored in the memory in the equipment and used for subsequent equipment operation. After it is confirmed that the data are normally recorded in the memory, the card is ejected.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－265516

(43)公開日　平成９年(1997)10月７日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｓ	
				Ｂ	
				Ｒ	
Ａ６３Ｆ　7/02	３３４		Ａ６３Ｆ　7/02	３３４	
Ｇ０７Ｆ　7/08			Ｇ０７Ｆ　7/08	Ｌ	

審査請求　未請求　請求項の数13　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平8－76201

(22)出願日　平成８年(1996)３月29日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　西岡　満
神奈川県川崎市幸区柳町70番地　東芝インテリジェントテクノロジ株式会社内

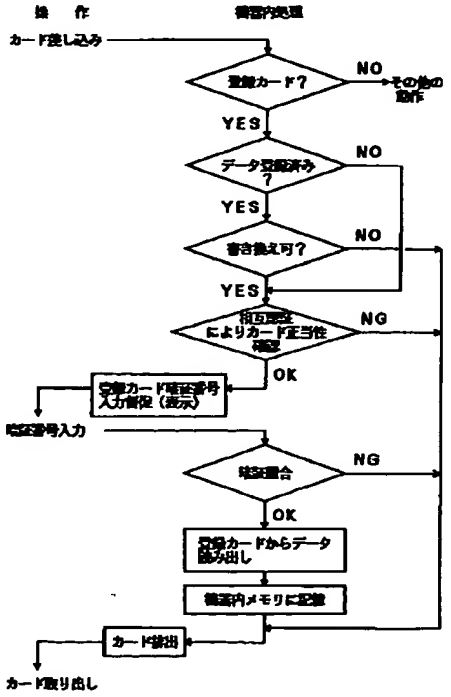
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　プリペイド用ＩＣカード処理装置

(57)【要約】

【課題】　ＩＣカードをプリペイドカード等として使用する場合の秘密鍵等の漏洩、盗難・不正使用等に関する問題を解決するＩＣカード処理システムを提供する。

【解決手段】　ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い装置と、前記取扱い装置の通常動作を可能とする動作データ、及び前記取扱い装置との間で相互に認証するための第１の相互認証プログラムを有する第１のＩＣカードと、前記取扱い装置が前記第１のＩＣカードとの間で相互に認証するための第２相互認証プログラムを有する第２のＩＣカードを具備する。



1

【特許請求の範囲】

【請求項1】　ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い手段と、
前記取扱い手段の通常動作を可能とする動作データを有する第1のＩＣカードと、
前記取扱い手段が前記第1のＩＣカードを照合するための照合データを有する第2のＩＣカードを具備し、
前記第2のＩＣカードから前記照合データが前記取扱い手段に登録され、登録された照合データを基に前記第1のＩＣカードの正当性が判断されることを特徴とするＩＣカード処理システム。

【請求項2】　ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い手段と、
前記取扱い手段の通常動作を可能とする動作データ、及び前記取扱い手段との間で相互に認証するための第1の相互認証プログラムを有する第1のＩＣカードと、
前記取扱い手段が前記第1のＩＣカードとの間で相互に認証するための第2相互認証プログラムを有する第2のＩＣカードを具備し、
前記第2のＩＣカードから前記第2の相互認証プログラムが前記取扱い手段に登録され、登録された前記第2の相互認証プログラム及び前記第1のＩＣカードが有する前記第1の相互認証プログラムを基に、前記第1のＩＣカード及び前記取扱い手段は互いに認証を確認しあうことを特徴とするＩＣカード処理システム。

【請求項3】　前記取扱い手段は、前記第1のＩＣカードにより登録されたデータを、登録から一定時間後に自動的に消去する手段を更に有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項4】　前記取扱い手段は、前記第1のＩＣカードにより登録されたたデータを、毎日一定時刻に自動的に消去する手段を更に有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項5】　前記取扱い手段は、前記第1のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が開かれたことを検出して前記格納手段に格納された前記動作データを消去する手段を有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項6】　前記取扱い手段は、前記第1のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が開かれたことを検出して前記筐体内部の時間・時刻データを無効化する手段を有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項7】　前記取扱い手段は、光センサにより前記蓋が開いたことを検出する手段を有することを特徴とする請求項5又は6記載のＩＣカード処理システム。

【請求項8】　前記取扱い手段は、前記第1のＩＣカードが有する前記動作データを格納する格納手段と、前記

2

取扱い手段の筐体が破壊されたことを検出して前記格納手段に格納された前記動作データを消去する手段を有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項9】　前記取扱い手段は、前記第1のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が破壊されたことを検出して前記筐体内部の時間・時刻データを無効化する手段を有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項10】　前記取扱い手段は、前記筐体部材内に張り巡らせた回路網が断たれることにより筐体の破壊を検出する手段を有することを特徴とする請求項8又は9記載のＩＣカード処理システム。

【請求項11】　前記取扱い手段は、ＩＣカードとの間で正当性確認情報を付加した電文を送受信することにより、前記ＩＣカードの正当性を確認する手段を有することを特徴とする請求項1～10のいずれか一項に記載のＩＣカード処理システム。

【請求項12】　前記取扱い手段は、複数の要因でＩＣカードの正当性を判断し、その判断結果により単なる不適合カードか偽造された不正カードかを判断する手段を有することを特徴とする請求項1～11のいずれか一項に記載のＩＣカード処理システム。

【請求項13】　前記取扱い手段は、不適合カードは排出し、不正カードは内部に取り込むかそのまま保持したまま他の機器へ発報する手段を有することを特徴とする請求項12記載のＩＣカード処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はＩＣカードを扱う装置に関し、特にプリペイドカード等の一部金額情報を書き換えて繰り返し使用できるＩＣカードを扱う機器における方式及び構造等に関する。

【０００２】

【従来の技術】現在多くのプリペイドカードは、ある金額の価値付けがされたカードを購入し、その額面だけ使い切ったらカード自体廃棄する使い切りタイプだが、一部金額情報を書き換えて繰り返し使用できるものもある。

【０００３】ＩＣカードをプリペイドカードとして使用する場合、機器におけるカード内の金額操作には増額（加算）と減額（減算）があり、加算を実行する機器は入金機として特別の扱いを受ける。即ち、自動式の場合、投入された現金に応じた金額をカードに書き込み内部に現金が蓄積される。又、係員等が現金を受け取り手操作により、支払われた現金に応じた金額をカードに書き込むため、厳格な操作資格管理が必要となる。従来、このような機器は次に示すような動作を行っている。

【０００４】（１．１）　秘密鍵等はメーカでプログラ

ムメモリに記録

ＩＣカードを扱う機器では、相互認証やデータの暗号化等に使用する暗号・復号化論理をプログラム化して機器内のＲＯＭ等のプログラムメモリに記録している。この様なデータはメーカでの機器製造時に記録されることになる。又ＩＣカードを扱う機器では、相互認証やデータの暗号化等に使用する秘密鍵をカードと相互に持ち合う場合が多い。この秘密鍵も、機器側のプログラムで扱われるため、機器内のＲＯＭ等のプログラムメモリに記録されている。

【０００５】（１．２）　カード販売機は電源とカードがあれば動作する

プリペイドカードの販売機としては、価値付け済みのカードを内部に蓄えておき「もの」として額面金額で販売するものと、価値付けしていないカードを内部に蓄えておき、投入金額に応じて都度価値付けして販売するものがある。又再度価値付け（増額）して再利用する運用形態の場合、単なる販売機ではなくカードへの入金機となるが、いずれも動作に必要な条件は「電源が供給されること」と「カードが供給されること」である。

【０００６】（１．３）　プリペイド残額の減算＝金額情報の書き換え

プリペイドカードにより物品を購入したりサービスを受けた際、物品の価額やサービスに応じた代価の支払いにあたる残額の減算は、カードに記録された金額情報をそれまでの値から、より小さい値（又は少ない金額、量を表す情報）への「書き換え」である。

【０００７】（１．４）　形状チェックと記録データ内容の照合により不適合カードを検出

機器に差し込まれたカードに対して、形状・電気特性等の物理的事項とカードに記録されているデータの照合により適合するカードがどうかが確認される。尚、実際には形状が違えば搬送・保持機構が正常に動作できないため、そのカードは受け付けられない。又、照合用の（キー）データに限らず、読出したデータの形式や値の範囲が規定外であった場合、処理を継続できないため、結果的に不整合カードを検出したことになる。このように、従来は積極的に不適合条件を検査するわけではない。

【０００８】（１．５）　不適合カードは排出する

差し込まれたカードに対して上記のような、物理的、論理的不適合が検出された場合、機器は単純に「使用できない」としてカードを受け付けずに排出する。

【０００９】

【発明が解決しようとする課題】ＩＣカードをプリペイドカードとして扱う従来の機器は次に示すような課題を有している。

（２．１）　秘密鍵等の漏洩

ＩＣカードを扱う機器では、相互認証やデータの暗号化等に使用する暗号・復号化プログラムやＩＣカードと相互に持ち合う秘密鍵は、機器内のＲＯＭ等のプログラム

メモリに記録されているため、機器の筐体を開いてプログラムメモリの内容を読出すことでこれらを入手することができる。又、これらの暗号・復号化プログラムや秘密鍵はメーカでの機器製造時にプログラムメモリに書き込まれるか、又はメーカでは機器ハードのみ製造しプリペイドシステムの管理会社において別に作成したプログラムＲＯＭを機器へ実装する等の手順があるが、基本的にエンドユーザの手に渡る前に動作可能な状態となるため、輸送途中で盗難されたり、倉庫等に保管している間に、次のような手段でプログラムメモリの内容を読出すことができる。

【００１０】具体的読出し方法として、プログラムや秘密鍵情報がＲＯＭに格納されているならば、このＲＯＭを取り外して市販のＲＯＭライタでダンプすることができる。又、制御回路にＩＣＥ(In Circuit Emulator) を接続すれば、上記のＲＯＭの内容は勿論、その他のメモリ素子等に記録されている内容でも自由に読出すことができる。

【００１１】これらの情報が入手できれば、同機能の機器やカードを偽造することができる。尚、秘密鍵については生データではなく、暗号化等が施された状態で機器のメモリに格納することが考えられるが、その機器の処理動作の一つとして秘密鍵を生データに戻す復号化が必ず存在するため、前述のＩＣＥを接続してプログラムを動作させればカードとのやりとりの経過処理において秘密鍵の値を得ることができる。この様な問題は、通信路を媒介として遠隔で相互に認証したりデータを秘匿化して交換するようなシステムで使用する機器においても内在している。

【００１２】（２．２）盗難・不正使用

プリペイドカードの販売機として、価値付け済みのカードを「もの」として額面金額で販売するものについては、販売機ごと盗まれても被害は内部に蓄えているカード（及び販売時投入された現金）だけだが、価値付けされていないカードを投入金額に応じて都度価値付けして販売するものや、カードを再利用する運用形態で入金機として機能するものの場合、カードが手に入ればその販売機を使用することで正当な代価を支払うことなく自由な金額で価値付けされたカードを作成することができる。

【００１３】（２．３）減算機の改造による不正使用

プリペイドカードによる物品の価額やサービスに応じた代価の支払いにあたる残額の減算は、カードに記録された金額情報の「書き換え」であるため、減算機能を持った機器（以下減算器）を改造することで前述の価値付けされていないカードが手に入れば前述同様に正当な代価を支払うことなく、自由な金額で価値付けされたカードを作成することができる。

【００１４】減算機は例えば無人稼動するものとしてはカード式電話機や飲料の自動販売機等があり、有人で人

手で操作するものとしてはＰＯＳレジ等に接続する汎用のプリペイドカード処理機等があるが、前者の場合やや大型ではあるが無人であり、後者の場合有人ではあるが小型なのでいずれも盗難の危険性は高いといえる。

【００１５】なお、上記の価値付けされていないカードを投入金額に応じて都度価値付けして販売するカード販機売機は、上記の様な不正使用方法が明確なため一般的に強固な盗難防止策がとられる。もちろん減算についても上記のような危険を内在していることが明確だが、市中での運用上販売機と同寺の盗難対策は困難といえる。

【００１６】（２．４）　不適合カードめ検査方法

従来は、差し込まれたカードに対して積極的に不適合条件を検査するわけではなく、形状・電気特性等の物理的事項とカードに記録されているデータの照合により適合するカートかどうかを確認しているに過ぎないため、たとえ高セキュリティのＩＣカードを使用したとしても偽造の危険性はまだ高いレベルにあるといえる。

【００１７】（２．５）　不正カード使用対策

従来、差し込まれたカードが不適合の場合、機器は単純に「使用できない」として受け付けずにカードを排出するだけなので、実際に偽造カード使用等の不正があつた場合にも、その使用者の特定やカードの回収はできない。

【００１８】従って本発明の目的は、ＩＣカードをプリペイドカード等として使用する場合の前述した秘密鍵等の漏洩、盗難・不正使用、減算機の改造による不正使用、不適合カードめ検査方法、不正カード使用対策に関する課題を解決するＩＣカード処理システムを提供することである。

【００１９】

【課題を解決するための手段】上記課題を解決するために本発明による第１のＩＣカード処理システムは、ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い手段と、前記取扱い手段の通常動作を可能とする動作データを有する第１のＩＣカードと、前記取扱い手段が前記第１のＩＣカードを照合するための照合データを有する第２のＩＣカードを具備し、前記第２のＩＣカードから前記照合データが前記取扱い手段に登録され、登録された照合データを基に前記第１のＩＣカードの正当性が判断される。

【００２０】更に、本発明による第２のＩＣカード処理システムは、ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い手段と、前記取扱い手段の通常動作を可能とする動作データ、及び前記取扱い手段との間で相互に認証するための第１の相互認証プログラムを有する第１のＩＣカードと、前記取扱い手段が前記第１のＩＣカードとの間で相互に認証するための第２相互認証プログラムを有する第２のＩＣカードを具備し、前記第２のＩＣカードから前記第２の相互認証プログラムが前記取扱い手段に登録され、登録された前記第２の相互認証プログラム及び前記第１のＩＣカードが有する前記第１の相互認証プログラムを基に、前記第１のＩＣカード及び前記取扱い手段は互いに認証を確認しあう。

【００２１】これにより上記（２．１）項で述べた秘密鍵等の漏洩に関する課題を解決することができる。又、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードにより登録されたデータを、登録から一定時間後に自動的に消去する手段を更に有する。

【００２２】更に、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードにより登録されたたデータを、毎日一定時刻に自動的に消去する手段を有する。

【００２３】これにより上記（２．１）項で述べた秘密鍵等の漏洩に関する課題、及び（２．２）項で述べた盗難・不正使用に関する課題を解決することができる。

又、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が開かれたことを検出して前記格納手段に格納された前記動作データを消去する手段を有する。

【００２４】又、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が開かれたことを検出して前記筐体内部の時間・時刻データを無効化する手段を有する。

【００２５】又、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体が破壊されたことを検出して前記格納手段に格納された前記動作データを消去する手段を有する。

【００２６】更に、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が破壊されたことを検出して前記筐体内部の時間・時刻データを無効化する手段を有する。

【００２７】これにより上記（２．１）項で述べた秘密鍵等の漏洩に関する課題、及び（２．３）項で述べた減算機の改造による不正使用に関する課題を解決することができる。

【００２８】又、本発明によるＩＣカード処理システムの前記取扱い手段は、プリペイドカード等として使用されるＩＣカードとの間で正当性確認情報を付加した電文を送受信することにより、前記ＩＣカードの正当性を確認する手段を有するこれにより上記（２．４）項で述べた不適合カードめ検査方法に関する課題、及び（２．５）項で述べた不正カード使用対策に関する課題を解決

することができる。

【００２９】又、本発明によるＩＣカード処理システムの前記取扱い手段は、複数の要因でＩＣカードの正当性を判断し、その判断結果により単なる不適合カードか偽造された不正カードかを判断する手段を有する。

【００３０】更に、本発明によるＩＣカード処理システムの前記取扱い手段は、不適合カードは排出し、不正カードは内部に取り込むかそのまま保持したまま他の機器へ発報する手段を有する。これにより上記（２．５）項で述べた不正カード使用対策に関する課題を解決することができる。

【００３１】

【発明の実施の形態】以下、この発明によるプリペイドカード用ＩＣカード処理装置の実施の形態を図面を参照して説明する。先ず始めに、機器の外観と機能構成ブロックの例をそれぞれ図１及び図２に示す。これは再度価値付け（増額）して再利用する運用形態のカード入金機４０である。この他に都度価値付けするカード販売機や、減算機能のみ持つ商品の販売機等があるが、本考案に関連する部分の最大構成を有するものとしてこれを示す。

【００３２】図１において、表示部４１はカード入金機４０を利用するための案内を表示する。カード差し込み口４３からカードは差し込まれ、金額選択ボタン４２により増額金額が入力され、金額投入・返却口４４から現金が投入又は返却される。テンキー４５は後述のキー登＊録カードのカードＩＤ等の値を管理者により入力するときに使用される。

【００３３】図２において、主制御部２は基本機能機能プログラムメモリ（ＲＯＭ）９に格納されたプログラムに従って、表示部４、入力部５、カード取扱い機構６、現金取扱い部７を制御する。主電源部３はＡＣ電源からＤＣ電源を発生し、主制御部２、ＲＯＭ９、表示部４、入力部５、カード取扱い機構６、現金取扱い部７に電源を供給する。バックアップ電源部８は主電源部３が動作していない時でも、常にメモリ１０ａ、１０ｂ、１０ｃに電源を供給する。

【００３４】本発明では従来の問題点を解決するための方策として次の５項目を説明する。

（３．１）登録カードによる主要データの登録

暗号・復号化プログラムや秘密鍵をプログラムメモリの内容を読み出すことにより入手することができないようにするため、機器への主要データ（主に機器動作用のデータ）のローディングは次のような項目を有する登録用ＩＣカードを使用する。

【００３５】（ａ）登録カード専用のフォーマット

（ｂ）登録カード専用のアクセス条件とキー値

（ｃ）登録カードごとに異なる所有者（使用者）暗証番号

このデータ登録カードの記録内容を表１に示す。

【００３６】

【表１】

データ・キー名称		内容の説明
カード内データアクセス用キー※	登録カードＩＤ	システムごとに異なる登録カードの身分証明番号 カード内で照合される読み出しできない照合用キー
	暗証番号	使用者が機器のテンキー等から暗証入力するキー カードごとに異なるいわゆる暗証番号
	相互認証用キー	本登録カードと機器の相互認証に使用されるキー このキー自体が照合されるのではない
機器へ登録するキーデータ	プリペイドカードＩＤ	実際の運用で使用されるカードのカードＩＤ
	相互認証用キー	プリペイドカード～機器の相互認証に使用されるキー
	正当性確認情報用キー	電文の正当性確認情報生成に使用されるキー
暗号ロジックまたはデータ		実際の運用で使用されるカードとのやりとりの中で必要とされる、機器側で実行される暗号処理のプログラム自体、又はそのプログラム動作に必要な主要データ

※照合用カード内データアクセス用キーの照合と相互認証処理が完了しない限り、他の読み出し・登録用のデータは読み出せない。

【００３７】このＩＣカードによるデータ登録は、機器をエンドユーザの元へ設置した後に実施することで、輸送中に盗難にあっても情報は漏洩しない。又、動作上の※重要データを有するカード、いわゆるキーカードの内容は機器のみが読出すことができるだけとし、それを使用するエンドユーザ自身に対しても知らせることなく運用

が可能である。尚、キーカードにより機器へ登録した各種の値を読出せない様にするための方法については後述する。

【００３８】この登録カードによる機器へのデータ登録操作と機器内処理の内容の例を図３に示す。先ず、操作者（管理者）により登録カードが機器に差し込まれる。機器側ではカードから得られる情報により、差し込まれたカードが登録カードかどうかを判定する。登録カード以外のカードが差し込まれた場合は適宜そのカードごとの処理へ移る。

【００３９】差し込まれたカードが登録カードであったならば、機器はそのカードで登録されるデータが既に登録済みであるかどうかを判定する。登録済みだった場合は差し込まれたカードのデータを新たに適用することで「書き換え」となるので、機器の設定として「書き換え」が許可されているかどうかを確認する。

【００４０】この機器の設定については製造時にシステムにあわせて固定値として設定しておいたり、製造後に登録カードによる本方法と同様の方法を含む種々の方法により設定することが考えられる。設定値としては、「書き換え不可」、「条件付き書き換え可能」、「無条件書き換え可能」等がある。「条件付き書き換え可能」の例として、金庫のダイヤルのように、カード挿入の回数及び時間間隔を設定することもできる。

【００４１】この設定で「書き換え」が許可された場合、及びデータが未登録の場合は次のステップへ移り、機器としてはカードの正当性を確認するべく相互認証をする。これがＯＫならば次は使用者の正当性確認のため、機器は操作表示部にメッセージを表示して操作者に対して暗証番号の入力を督促する。

【００４２】操作者によりその登録カードの暗証番号が入力されると機器はカードに対してその番号を照合し、ＯＫになってはじめて登録データの読出しに移る。この暗証照合がＮＧの場合、機器側の処理として登録データを読出しに行かないことは勿論だが、仮にこの状態でカードからデータを読出そうとしてもカードは暗証照合がＯＫとなっていないのでデータを出力しない。又、上記相互認証において、カード側が機器を正当な相手と判定していない場合は、例え暗証照合がＯＫとなってもカードはデータを出力しない。これらにより偽造された機器では登録データを読出すことはできない。

【００４３】このようにして読出された登録データは機器内のメモリに記憶されて、以降の機器動作に使用される。又、機器内のメモリに正常に記録されたことが確認された後、機器はカードを排出し操作者がこれを抜き取って保管する。

【００４４】次にこの様な機器の製造から運用に至るサイクルの例を、プリペイドシステム管理会社から機器供給を受けて運用するパチンコ店、ゲームセンタ等の遊技場での使用を例に図４に示す。

【００４５】先の登録操作と機器内処理の実施例では単純に一種類のカードでデータ登録する例を示したが、この実施例では実際のデータ（機器動作用データ）を登録するためのカードを「データ登録カード」として、この「データ登録カード」の使用を可能とするための各種のキーの値を設定する「キー登録カード」の２種類を使用している。

【００４６】「キー登録カード」で登録するキーとしては、上記登録操作と機器内処理の実施例で示した相互認証で使用するキーの他、登録カードであることを示すための照合用データであるカードＩＤ（キー）等がある。この２種類のカードの記録内容をそれぞれ表２及び表３に示す。

【００４７】

【表２】

データ・キー名称		内容の説明
カード内データアクセス用キー※	キー登録カードＩＤ	システムごとに異なるキー登録カードの身分証明番号 この値だけは本カードの使用前に機器に登録する
	暗証番号	使用者が機器のテンキー等から暗証入力するキー カードごとに異なるいわゆる暗証番号
	相互認証用キー	本登録カードと機器の相互認証に使用されるキー このキー自体が照合されるのではない
機器へ登録するキーデータ	データ登録カードＩＤ	データ登録カードのカードＩＤ
	相互認証用キー	データ登録カード～機器の相互認証に使用されるキー
	正当性確認情報用キー	データ登録カードと機器間の電文の正当性確認情報生成に使用されるキー

※照合用カード内データアクセス用キーの照合と相互認証処理が完了しない限り、登録用キーデータは読み出せない。

【００４８】　＊　＊【表３】

データ・キー名称		内容の説明
カード内データアクセス用キー※	データ登録カードＩＤ	システムごと異なるデータ登録カードの身分証明番号 キー登録カードにより登録される
	暗証番号	使用者が機器のテンキー等から暗証入力するキー カードごとに異なるいわゆる暗証番号
	相互認証用キー	本登録カードと機器の相互認証に使用されるキー このキー自体が照合されるのではない
正当性確認情報用キー		
機器へ登録するキーデータ	プリペイドカードＩＤ	実際の運用で使用されるカードのカードＩＤ
	相互認証用キー	プリペイドカード～機器の相互認証に使用されるキー
	正当性確認情報用キー	電文の正当性確認情報生成に使用されるキー
暗号ロジックまたはデータ		実際の運用で使用されるカードとのやりとりの中で必要とされる、機器側で実行される暗号処理のプログラム自体、又はそのプログラム動作に必要な主要データ

※照合用カード内データアクセス用キーの照合と相互認証処理が完了しない限り、登録用データは読み出せない。

【００４９】キー登録カードは次のような運用が考えられる。

（ａ）例えば一店舗を一つのシステムと見なし、１システム（各店）ごとに１枚作成し管理会社が保管・使用する。

【００５０】（ｂ）基本的に機器の設置時、その店のシステムの初期設定として管理会社がこのカードを使用して、そのシステム（店舗）で使用するデータ登録カードのアクセスキーを機器へ登録する際に使用する。

【００５１】（ｃ）事故等でその店舗の機器のキーデー※50※タが消えてしまった場合や、データ登録カードのアクセスキーの値にに変更が生じた場合には、管理会社が出向いてそのキーを機器へ再登録する。

【００５２】（ｄ）キー登録カード自体の暗証番号の他、データ登録カード使用に先だって暗証番号を入力しないとデータ登録カードが使用できないようにすることもできる。

【００５３】又、データ登録カードは次のような運用が考えられる。

（ａ）例えば一店舗を一つのシステムと見なし、１シス

テム（各店）．ごとに1枚～数枚作成し、店舗のシステム管理者が保管・使用する。

【0054】（b）基本的に毎朝、昨夜（昨営業日）の深夜0時で自動消去されてしまった機器の動作用データを再登録する際に使用する。これにより機器は当日の深夜0時まで使用可能となる。

【0055】（c）データ登録カード自体のID番号の他、データ登録カード使用に先だって暗証番号を入力しないと登録カードが使用できないようにすることもできる。図4に示すこれらのカードを使った機器の使用例の流れは次のようになる。

【0056】機器はメーカにて、カードのハンドリング、表示、通信制御と、カードを使った各種処理の基本部分を搭載した機器として製造される。機器はメーカから管理会社へ納入されるか、管理会社からの指示により設置場所へ直接納入され、管理会社の担当者立ち会いのもとユーザの遊技場（店舗）に設置される。このとき、管理会社の担当者がキー登録カードを使用して、データ登録カードのアクセスキーデータを機器へ登録する。このキー登録カードを使用するには、機器側にキー登録カードのカードIDが登録されている必要があり、これについては固定値として製造時に機器に登録してしまうか、機器のテンキーから管理会社の担当者が入力する等が考えられる。又、このとき店舗ごとに記録データの異なるデータ登録カードをユーザ側へ引き渡し、機器の運用管理は遊技場に任される。

【0057】店側ではデータ登録カードを使って、このカードを管理する責任者（システム管理者）により、機器動作用のデータを機器へ登録する。このデータ登録が完了した後、機器は実際に使用可能となる。

【0058】ここで、本実施例では3．2項として以下に示される「キーカードによる使用時間延長」の機能も盛り込んでいる。即ち、店のシステム管理者がデータ登録カードで登録したデータが機器内部の時計により、登録後の一定時間か、時刻としての一定時刻に自動消去するようにしておき、データ登録カードを使用して再度登録しなくては使用不可能となるように設定できる。4図では後者の一定時刻として深夜0時でデータが消去され、翌朝又は翌営業日開店前に再登録するものとしている。このような運用により、店舗が無人となる深夜や休日まで使用できない状態となり、盗難されてもデータ登録カードがなければ不正使用されることはありえない

（3．2）データ登録カードによる使用時間延長（カード販売機について）

価値付けされていないカードを投入金額に応じて都度価値付けして販売するものや、カードを再利用する運用形態で入金機として機能する機器において、価値付けされていないカードが手に入っても、その販売機を使用して正当な代価を支払うことなく自由な金額でカードに価値付けできないようにするために、一定時間に一回、使用許可キーカードを差し込まないと自動的に使用不能とする。

【0059】この方式の実施例は、データ登録カードを使用許可を与えるキーカードとして利用し、玉貸金額書込機内のカレンダの日付が変わると書込機内の各種キーの値が自動消去される例を「3．1登録カードによる主要データの登録」の運用例として記載している。

【0060】（3．3）　開蓋・破壊時データ消去

以下の手法により、機器のケースを開く等すると動作に必要な機器内の主要データが消云される。

【0061】動作に必要なデータの主要部分はROMには載せずにハードウェアの完成後外部からRAM等の揮発性のメモリ部分へローディングするものとし、ケースを開いたり破壊したりするとこのメモリの内容の保持動作（回路）が中断（切断）しメモリ内のデータを消すことで、それ以降は動作不能とする。

【0062】この方式の実施例は運用例として「データ登録カード」とそのカードのアクセス用キーを登録する「キー登録カード」により、機器へ動作に必要なデータを登録する部分を「3．1　登録カードによる主要データの登録」の運用例の中に記載している。

【0063】以下に構造案の実施例を示す。

（a）蓋開センサ／スイッチ方式

この筐体構造の断面図を図5に示す。筐体の蓋20が開かれると解放する光センサスイッチSW1又は機械スイッチSW2、SW3を介して、バックアップ電池8による電源が供給されることで静的（Static）に内容が保持されている揮発性メモリ（SRAM等）10にデータを記録することで、蓋20が解放されスイッチが解放された瞬間にバックアップ電源が断たれメモリ内容は揮発する。

【0064】（b）入射光センサ方式

この筐体構造の断面図を図6に示す。光が入射すると回路を解放する光センサスイッチSW4、SW5を介してバックアップ電池8による電源が供給されることで静的に内容が保持されている揮発性メモリ10にデータを記録することで、蓋20が解放され光センサスイッチに光が入射した瞬間にバックアップ電源が断たれメモリ内容は揮発する。

【0065】（c）筐体回路パターン方式

この筐体構造の断面図を図7に示す。図7（b）に示すように、筐体の素材内に巡らされた回路網を通してバックアップ電池8による電源が供給されることで静的に内容が保持されている揮発性メモリ10にデータを記録することで、筐体の一部が破壊され回路網が途絶した瞬間にバックアップ電源が断たれメモリ内容は揮発する。筐体全体に回路網を通す構造が理想だが、ここでは蓋部材に回路網を通し基板上のコネクタで接続する方式例の筐体構造を示す。

【0066】以上の実施例は全て、筐体を開こうとした

際に揮発性メモリ１０のバックアップ電源を断つ方式だが、これらの蓋・筐体を開いたことを検出する手法を利用し、次のようにメモリのデータを消すことも可能である。尚、これらを複合して使用することも十分考えられる。

【００６７】（ｄ）ＤＲＡＭ保持動作中断方式
この方式の動作の流れを第８図に示す。データを動的（Ｄｙｎａｍｉｃ）にメモリ保持動作をする形式のメモリ（ＤＲＡＭ等）に記録し、蓋・筐体が開かれたことをきっかけにこのメモリ保持動作を中断する。具体的にはＤＲＡＭ１０のメモリ保持動作（リフレッシュ）に不可欠なクロック信号の供給を主制御部２から制御できる回路構成としておき、蓋・筐体が開かれたことをスイッチ、センサ等で検出したらこのクロック信号を止める割り込み処理を起動することで実現できる。

【００６８】（ｅ）消去プログラム起動方式
この方式の動作の流れを図８に示す。上記の様なバックアップ電源に関する処置をしていない、常にバックアップされ続けるメモリにデータを記録し、蓋・筐体が開かれたことをきっかけにこのデータを消去するプログラムを強制起動する。具体的には、消去すべきデータが格納されているメモリに対してスペースやＮＵＬＬ等意味のないダミーデータを書き込む割り込み処理を用意しておき、蓋・筐体が開かれたことをスイッチ、センサ等で検出したらこの割り込み処理を起動することで実現できる。

【００６９】以上は登録データを消去することを主旨に説明したが、この手法は（３．２）に示した「使用時間延長」の処理で使用する機器内の時計が進まないように改造することの防止にも応用できる。即ち機器内の時計が進まないように改造することでキーカードによる時間延長を不要とし、永続的に使用できるようにすることができるため、蓋が開かれたり筐体が破壊された場合、時間・時刻データを無効化することで不正使用を防ぐことになる。

【００７０】（３．４）電文正当性確認
秘密鍵をカードと機器で持ち合い、相互に共有する何らかのデータを秘密鍵を用いて暗号化し、暗号化されたデータを正当性確認情報として電文の一部として含め、その電文が正当な相手から送られてきたものであることを正当性確認情報の内容により、カードと機器双方が確認する。

【００７１】機器から送られてきた電文のカード側での確認は、主として偽造された機器による正当なカードに対する金額の書込（増額）を防止し、カードから送られてきた電文の機器側での確認は、主として偽造されたカードによる正当な機器での買い物（購入）を防止する。又、機器側がカードを不正と判定した場合、そのままカードを保持し警報を発したり、機器内部に回収することも可能である。

【００７２】以下にカードと機器双方における正当性確認手順の例を示す。又、これらを複合して各々で電文の正当性を確認するやりとりの例を図１０に示す。図１０はカードの残高を減額し商品を販売するような運用形態を示す。このような処理の使用例としては、カード側での機器からのコマンド電文の正当性確認は偽造された入金機による正規カードへの入金を防止し、機器側でのカードからの実行結果通知電文の正当性確認は偽造カードによる商品等購入を防止する効果が狙いとなる。従って図１０のように相互に正当性確認を実行することは少ないと考えられる。即ち、偽造カードに正規の入金機で現金を支払って入金することも、商品販売に使用する減額機器を偽造することも、いずれも（不正な）利益は生み出さないためである。しかし、使用者が偽造カードと知らない場合等に後述の３．５に示す様な不正カードを回収し、出所を探るためには有効でる。尚、金額書き換えコマンドの使用に至る前に、カードと機器相互に正当な相手であることを確認するための「相互認証」を実行する後述の３．５に示す様な運用形態も考えられ、本実施例と併用することも可能である。

【００７３】次に図１０の動作によるカード側での正当性確認を説明する。以下の手順で機器からの金額書き換えコマンド自体の正当性を確認し、正当と判定されたときのみカードは金額書き換えを実行する。

【００７４】（ｓｔＡ）　金額書き換えに先立ち機器がカードに対して乱数出力を要求しカードがこれに応える。

（ｓｔＢ）　機器側では取得した乱数を基にこれから書き込もうとする書込日、書き込み金額を秘密鍵で暗号化する（この暗号化されたデータが正当性確認情報である）。

【００７５】（ｓｔＣ）　機器からカードへステップｓｔＢで生成したデータを金額書き換えコマンド電文の一部として送信する（書込日、更新金額も電文に含めて送る）。

【００７６】（ｓｔＤ）　金額書き換えコマンド電文を受けたカードは先に送出した乱数を基に、内部で同様の暗号化により正当性確認情報を生成し、電文内の同データと比較することで機器からの電文の正当性を確認し、照合ＯＫのときにのみカードは金額書き換えを実行する。

【００７７】（ｓｔＥ）　照合がＯＫでなかった場合、カードは機器に対して処理実行否定通知を送る。この例は減額機器の場合を示しているが、カード側での機器からの電文の正当性確認情報の照合（ｓｔＤ）は、偽造された入金機（増額機器）による正規カードへの入金を防止することができる。

【００７８】次に図１０の動作による機器側での正当性確認を説明する。上記カード側での正当性確認のステップｓｔＤにおいて、カード側で電文を正当と判定し金額

書き換えが実行されると、処理結果の如何に関わらずカードは機器に対して実行結果通知レスポンス電文を返す。このとき次の手順によりカードからの結果通知電文自体が正当なものであるかどうかを確認し、正当と判定されその内容が金額書き換え処理が正常終了を示すときのみ機器はカードに対する処理を実行する。

【００７９】（ｓｔＦ）　金額書き換えを実行したカードは、金額書き換えコマンド電文の一部として機器から受け取つた現在時刻、引き去り金額等を、暗号化用秘密鍵を用いてカード内で暗号化する（この暗号化されたデータが正当性確認情報）。

【００８０】（ｓｔＧ）　カードから機器へステップｓｔＦで生成したデータを、書き込みコマンド電文の実行結果通知（応答）電文の一部として送信する。

（ｓｔＨ）　実行結果通知（応答）電文を受けた機器は、内部で同様に正当性確認情報を生成する。

【００８１】（ｓｔＩ）　生成した正当性確認情報と電文内同データと比較することで機器かの電文の正当性を確認し、照合ＯＫのときにのみ機器はそのカードを使用して所望される動作の最終段階（例えばプリペイド自販機による商品購入時の商品の送出）を実行する。

【００８２】（３．５）　不正カード使用発報

「相互認証」や「実行結果（応答）電文正当性確認」により、使用されたカードが不正カードであると判定された際、機器はそのカードを内部に保持したまま機器の管理者側（ホスト）へ通知（即時発報）する。これにより使用された不正カードを回収したり、使用者を特定することができる。具体的動作の流れを図１１に示す。又、図１２に複数の機器３０とそれにオンライン接続されたホスト３１構成されるシステムを示す。

【００８３】機器はカードが差し込まれるとカードを活性化する。活性化時に機器が受け取るカードの初期応答（アンサトゥリセット）については、別種の用途のカードでは機器側で所望の値ではない場合も多く、単なる不適合カードとして排出すればよい。この初期応答が所望の値だった際、機器はカードＩＤの照合に移る。カードＩＤについては用途・システムにより様々な値とすることが当然であり、照合ＮＧの場合やはり単なる不適合カードとして排出すればよい。

【００８４】カードＩＤの照合がＯＫだった場合、引き続き相互認証の処理に移る。相互認証についてはカードＩＤが一致した場合、基本的に（カードやデータが壊れていない限り）不成立となることはなく、不成立の場合それはほぼ不正カードであると判断して間違いない。この不成立の内容には、相互認証機能がない、相互認証に使用される乱数生成ロジックが異なる、同一のロジックでも使用するキー値が異なる、等が考えられる。このとき機器はそのカードを内部に保持したまま使用者には判らないように不正カードが使用されたことをオンラインでホストへ即時に発報する。

【００８５】相互認証が正常に終了した場合、引き続き金額書き換え処理に移る。この金額書き換えでは、電文の正当性確認を行なうが、相互認証までもが正常に終了した場合、カードＩＤが一致しただけより更に正当性確認情報が不整合となることはなく、不整合の場合それはほぼ不正カードであると判断して間違いない。このとき機器はそのカードを内部に保持したまま使用者には判らないように不正カードが使用されたことをオンラインでホストへ即時に発報する。尚、この不整合の原因には、上記相互認証が不成立となる要因と同様、不正カードに、機能がない、ロジックが異なる、キー値が異なる等がある。

【００８６】３．１に示したプリペイドシステム管理会社から機器供給を受けて運用するパチンコ店、ゲームセンタ等の遊技場の例においては、発報を受けたホストは該当する機器を特定する情報を表示するので、係員は発報した機器へ出向きそのカードを回収するとともに、使用者に事情を聞くといった運用が可能である。又、不正カードを機器の内部に回収してしまうことは３．１の例に限らず適用可能である。

【００８７】

【発明の効果】本発明により、プリペイド用ＩＣカードと処理装置を偽造・変造されにくくできる。即ち、プリペイド用ＩＣカード等の高セキュリティ化されたカードのセキュリティレベルを機器やデータ管理面で低下することがないだけでなく、システム全体をより高セキュリティ化することができる。

【図面の簡単な説明】

【図１】ＩＣカード入金機の外観を示す。

【図２】ＩＣカード入金機の機能構成を示すブロック図。

【図３】本発明の登録カードによる機器へのデータ登録操作と機器内処理を示すフローチャート。

【図４】プリペイド用ＩＣカード取扱い機器の製造から運用に至るサイクルの例を示すフローチャート。

【図５】蓋開センサ／スイッチ方式の筐体断面図。

【図６】入射光センサ方式の筐体断面図。

【図７】筐体回路パターン方式の筐体断面図。

【図８】ＤＲＡＭ保持動作中断方式の動作を示すフローチャート。

【図９】消去プログラム機動方式の動作を示すフローチャート。

【図１０】ＩＣカードと機器双方で電文の正当性を確認するやりとりの例を示す図。

【図１１】不正カード使用時の発報処理動作を示すフローチャート。

【図１２】機器とホストをオンライン接続した構成を示す図。

【符号の説明】

２…主制御部

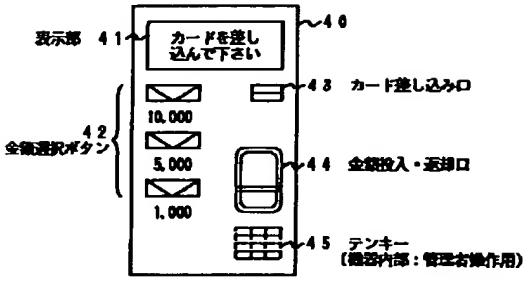
19

3…主電源部
4…表示部
5…入力部
6…カード取扱い機構
7…現金取扱い部
8…バックアップ電源部

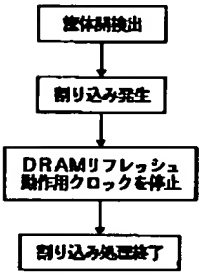
20

9…プログラムメモリ
10a…ワーキングメモリ
10b…暗号機能プログラムメモリ
10c…キーデータメモリ
40…カード入金機

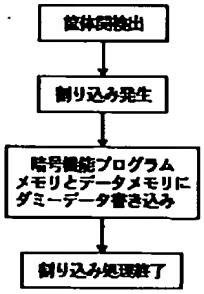
【図1】



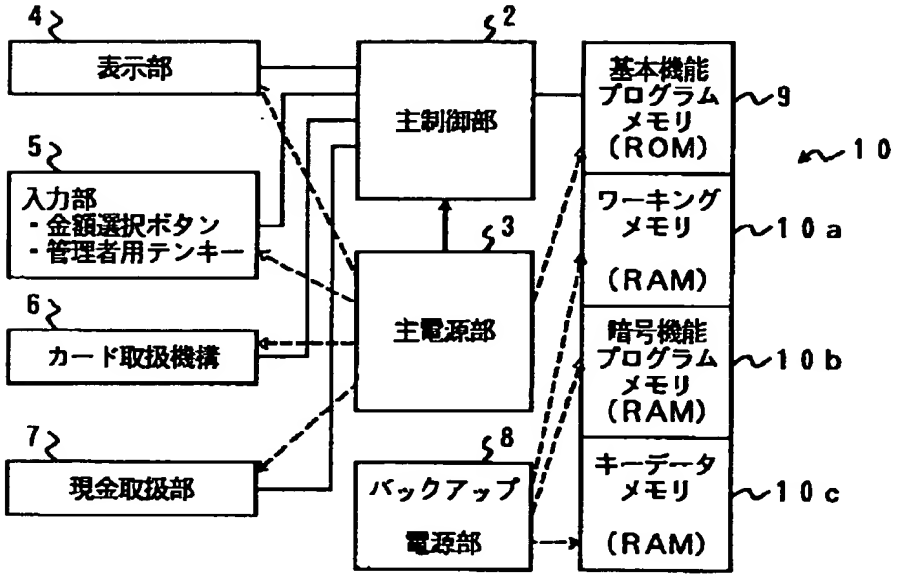
【図8】



【図9】

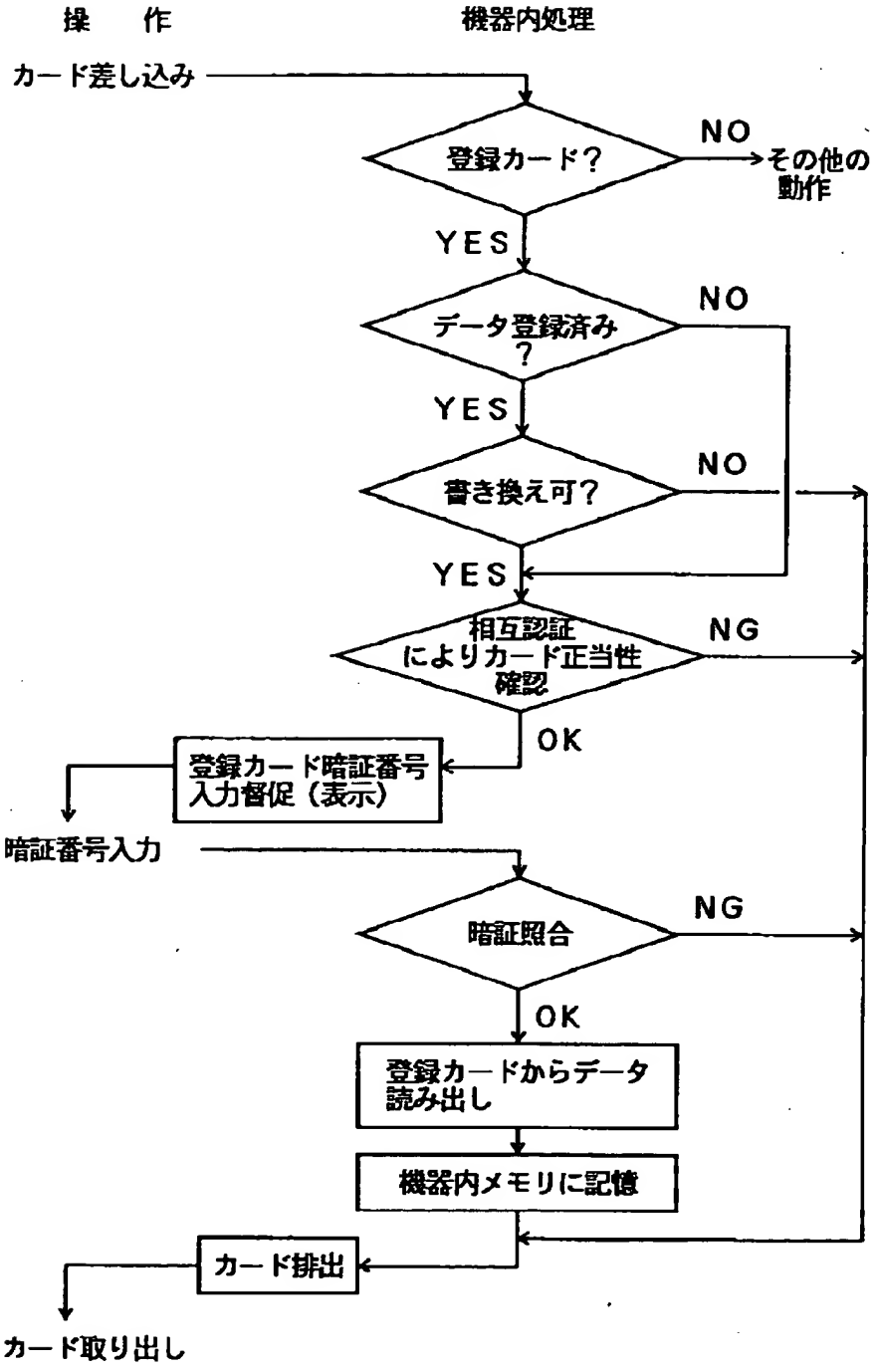


【図2】

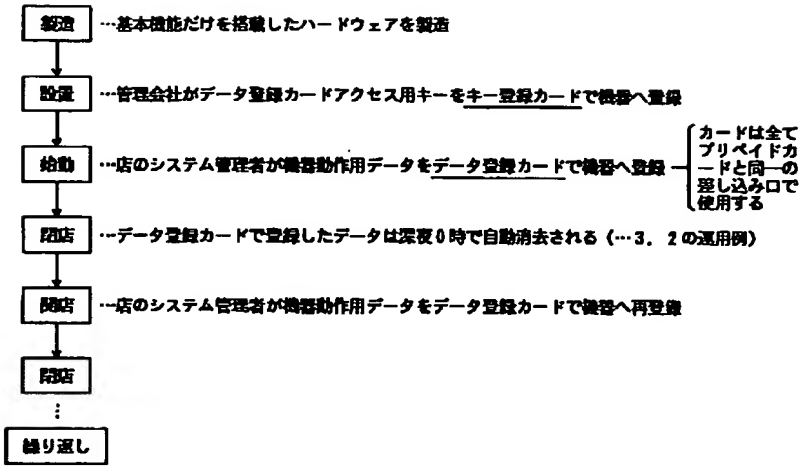


［ ——— ：制御　　------ ：電源］

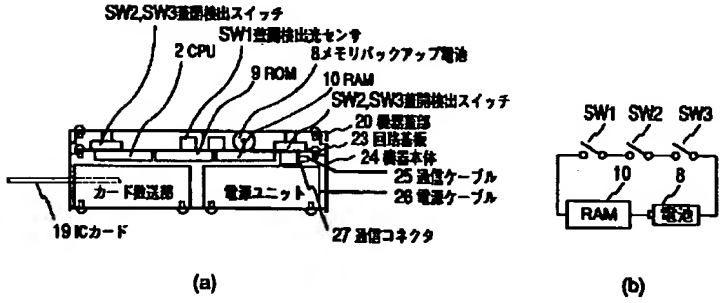
【図3】


操　作
機器内処理
カード差し込み
登録カード？
NO
その他の動作
YES
データ登録済み？
NO
YES
書き換え可？
NO
YES
相互認証によりカード正当性確認
NG
OK
登録カード暗証番号入力督促（表示）
暗証番号入力
暗証照合
NG
OK
登録カードからデータ読み出し
機器内メモリに記憶
カード排出
カード取り出し

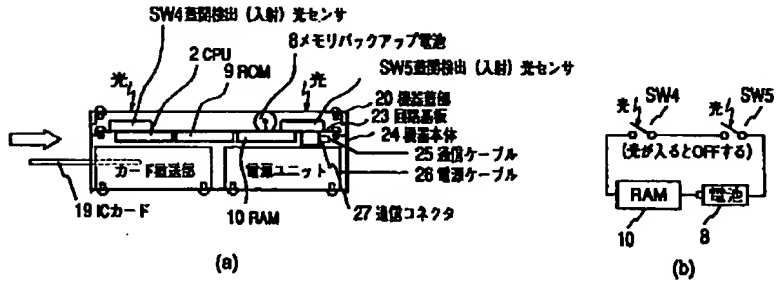
【図4】


製造
…基本機能だけを搭載したハードウェアを製造
設置
…管理会社がデータ登録カードアクセス用キーをキー登録カードで機器へ登録
始動
…店のシステム管理者が機器動作用データをデータ登録カードで機器へ登録
カードは全てプリペイドカードと同一の差し込み口で使用する
閉店
…データ登録カードで登録したデータは深夜0時で自動消去される（…3．2の運用例）
開店
…店のシステム管理者が機器動作用データをデータ登録カードで機器へ再登録
閉店
繰り返し

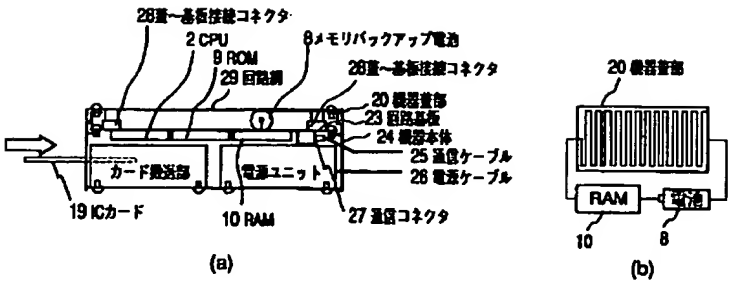
【図5】


SW2,SW3蓋開検出スイッチ
SW1蓋開検出光センサ
2 CPU
8メモリバックアップ電池
9 ROM
10 RAM
SW2,SW3蓋開検出スイッチ
20 機器蓋部
23 回路基板
24 機器本体
25 通信ケーブル
26 電源ケーブル
カード読込部
電源ユニット
19 ICカード
27 通信コネクタ
(a)
SW1 SW2 SW3
10
8
RAM
電池
(b)

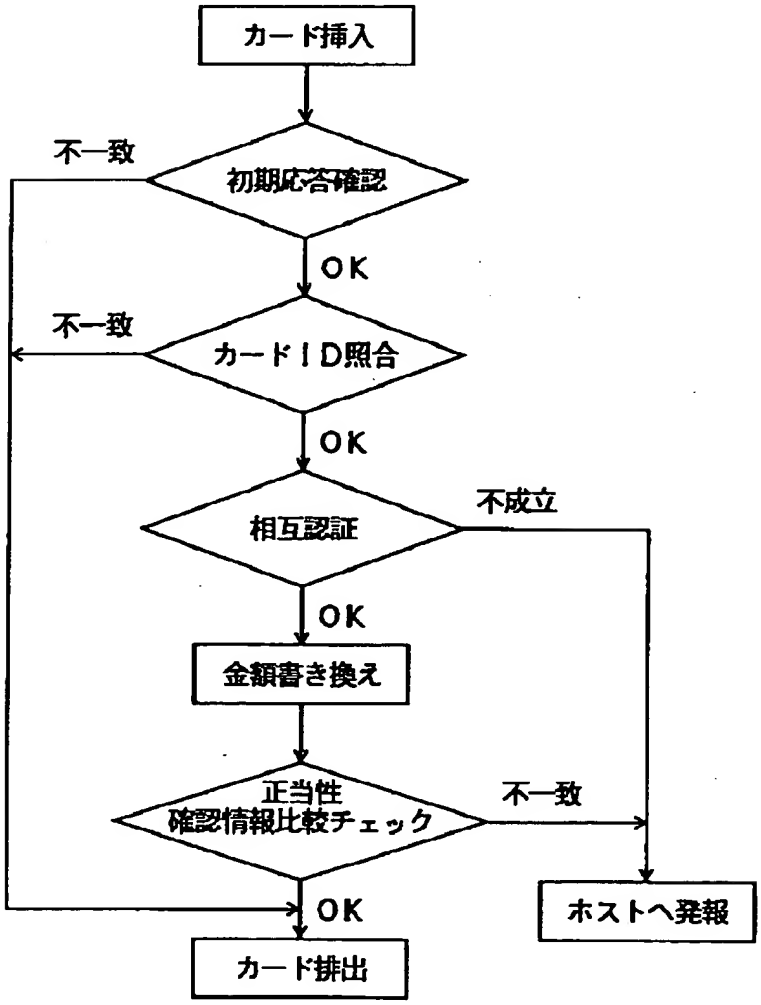
【図6】


SW4蓋開検出（入射）光センサ
8メモリバックアップ電池
2 CPU
9 ROM
光
光
SW5蓋開検出（入射）光センサ
20 機器蓋部
23 回路基板
24 機器本体
25 通信ケーブル
26 電源ケーブル
カード読込部
電源ユニット
19 ICカード
10 RAM
27 通信コネクタ
(a)
光
SW4
光
SW5
（光が入るとOFFする）
RAM
電池
10
8
(b)

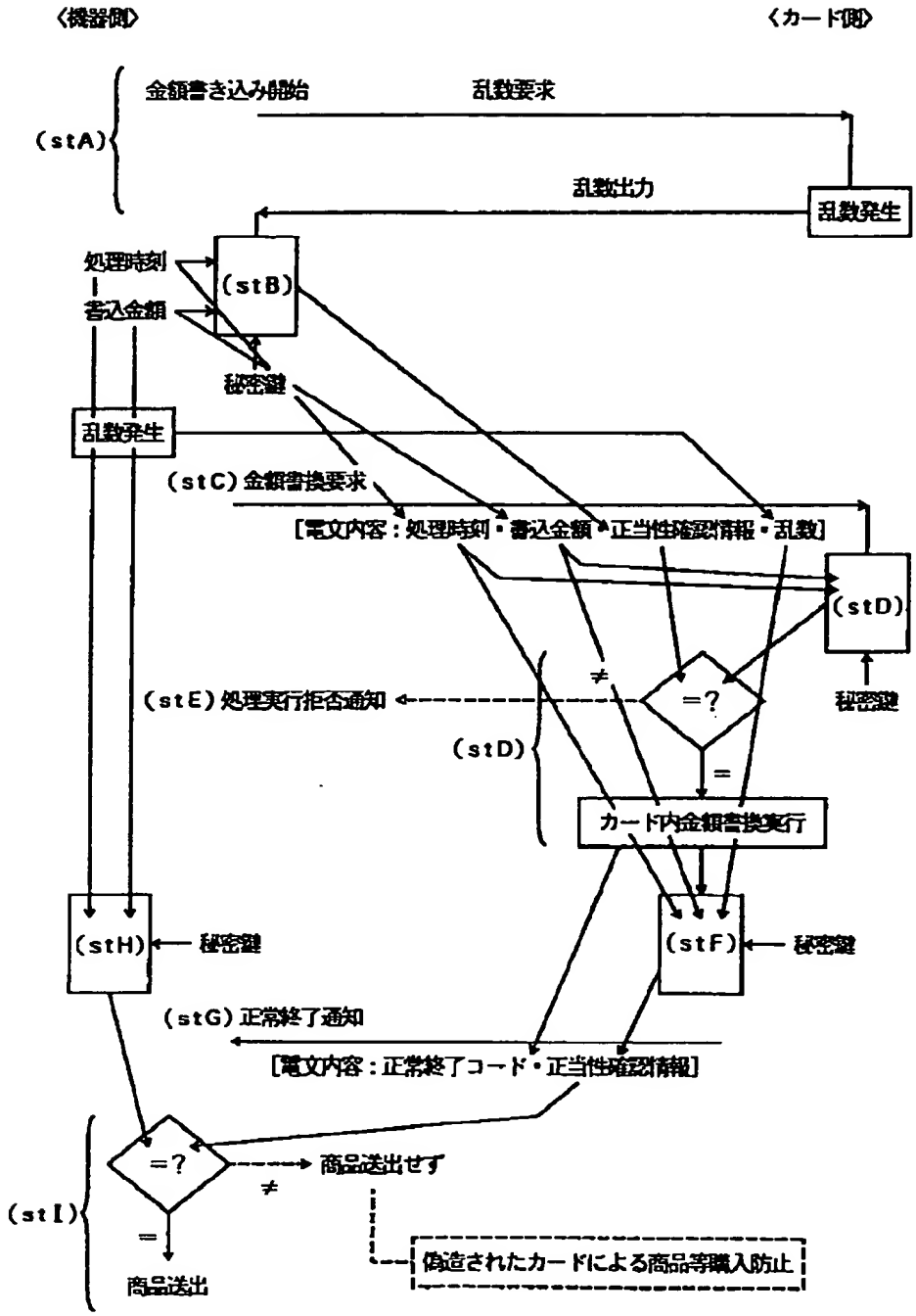
【図7】


2 CPU
9 ROM
29 回路網
20 機器筐体
23 回路基板
24 機器本体
25 通信ケーブル
26 電源ケーブル
カード搬送部
電源ユニット
19 ICカード
10 RAM
27 通信コネクタ
(a)
20 機器筐体
RAM
10
8
(b)

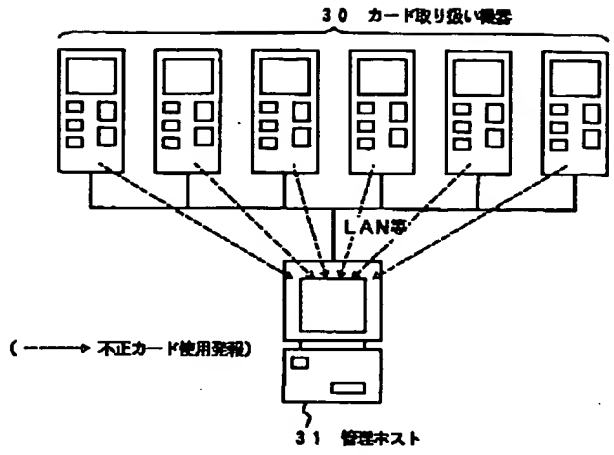
【図11】


カード挿入
初期応答確認
不一致
OK
カードID照合
不一致
OK
相互認証
不成立
OK
金額書き換え
正当性
確認情報比較チェック
不一致
OK
ホストへ発報
カード排出

【図10】


〈機器側〉
〈カード側〉
(stA)
金額書き込み開始
乱数要求
乱数出力
乱数発生
処理時刻
書込金額
(stB)
秘密鍵
乱数発生
(stC) 金額書換要求
[電文内容：処理時刻・書込金額・正当性確認情報・乱数]
(stD)
秘密鍵
≠
=?
(stE) 処理実行拒否通知
(stD)
=
カード内金額書換実行
(stH)
秘密鍵
(stF)
秘密鍵
(stG) 正常終了通知
[電文内容：正常終了コード・正当性確認情報]
(stI)
=?
商品送出せず
≠
=
商品送出
偽造されたカードによる商品等購入防止

【図12】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI		技術表示箇所
G07F 7/12			G07F 7/08	S	
				C	